

Re: group opinion requested

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2005-01/2376.html>

From: Marcia (*mkp_at_1248.com*)

Date: 01/09/05

Date: Sun, 9 Jan 2005 14:51:31 -0500

Thanks for replying again. I and PSS didn't think it was compromised prior to this most recent event. We both believed the main problem being due to the .NET patch.

The ports I have opened are 25, 1723, 3389, 443, 4125, and 80 on the router. We use OWA, RWW, our own smtp email, and the Internet. Pretty basic.

When I asked PSS on Friday if she thought we were compromised, her initial answer was no. She believes someone ran a port scan and found port 25 open and spammed it with NDR's.

I don't know. I've never experienced this before with any of my clients.

Thanks.

Marcia

"Marina Roos [SBS-MVP]" <marina@roos.nodontwantspam.nl.com> wrote in message news:Og2j%23Ko9EHA.1392@tk2msftngp13.phx.gbl...

> *Hi Marcia,*

>

> *If you suspect a security issue, you can call the MS Security Team. This is*

> *free. They will check your server thoroughly. Did/do you have any suspicion*

> *at all that the server might have been compromised? Which ports are open inbound?*

>

> --

> *Regards,*

>

> *Marina*

> *Microsoft SBS-MVP*

> *One of the Magical M&M's*

>

> *"Marcia" <mkp@1248.com> schreef in bericht*

> *news:u3iK3Ho9EHA.2196@TK2MSFTNGP11.phx.gbl...*

> > *Hi! I value the expertise from this news group, I wanted to seek your
> > opinion on a security issue.*
> >
> > *We had problems with our server just before Christmas and replaced the
> > motherboard and had to completely uninstall/reinstall IIS and Exchange
> > with
> > the PSS. I'm still not convinced that the motherboard was bad, but it
is
> > now in the hands of the vendor under warranty repair.*
> >
> > *PSS and I had the server back up and operational after several days.*
> >
> > *On the 4th, we started receiving tons of NDR's. In the 7th, the server
> > slowed down to a near stop. I contacted PSS again only to find that we
> > were
> > relaying via our loopback ip. Also, dns entries were in the Default
SMTP
> > Virtual Server of our ISP. These were not added there when PSS and I
> > completed the initial round.*
> >
> > *We removed the loopback ip from our relay list and the dns IP's from the
> > Def. SMTP Vir. Server. Now email is functioning again.*
> >
> > *My big question is this: We thought we had the server completed when
this
> > issue appeared on the 7th. How do we know if other issues will randomly
> > pop
> > up and if we weren't hacked with a backdoor? In otherwords, the initial
> > down time was caused by something (I don't believe it was hardware).*
How
> > *do
> > I know if it was an attack and if the loopback/isp dns's were the result
> > of
> > a backdoor?*
> >
> > *Has anyone ever contacted MS Security group for PSS? I assume they have
> > the
> > tools and experience to maybe answer this question.*
> >
> > *I don't want anything else to come up and I'm seriously wondering if
> > reformatting and starting over is the only secure way. I know that is
> > rash--and I haven't decided to do that yet.*
> >
> > *I am merely querying the opinions of this group.*
> >
> > *And again, as always, I appreciate you more than the word "Thanks" can
> > ever
> > convey. The generosity and knowledge of this group is overwhelming. I
> > doubt that I'll ever be able to provide the knowledge level that I
> > recieve--I can only keep trying.*
> >

microsoft.public.windows.server.sbs: Re: group opinion requested

> > *Marcia*

> >

> >

>

>